TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Emilia Kaikkonen

Lineaarisista taikaneliöistä ja niiden konstruoinnista

Informaatiotieteiden yksikkö
Matematiikan maisteriopinnot
Kesäkuu 2014

Tampereen yliopisto

Informaatiotieteiden yksikkö

KAIKKONEN, EMILIA: Lineaarisista taikaneliöistä ja niiden konstruoinnista

Pro gradu -tutkielma, 25 s.

Matematiikan maisteriopinnot

Kesäkuu 2014

Tiivistelmä

Tässä pro gradu -tutkielmassa tutustutaan lineaarisiin taikaneliöihin ja lineaaristen taikaneliöiden konstruointiin. Tutkielman sisällön ymmärtämisen kannalta keskeisimmät aihealueet käsitellään vain kertauksenomaisesti omassa luvussaan, sillä lukijalta odotetaan aiempaa tietämystä lineaarialgebrasta ja algebrasta. Äärellisiin kuntiin, vektoriavaruuksiin ja lukujärjestelmiin pohjautuva luku toimii samalla matemaattisen ajattelun herättäjänä, josta lukija voi sujuvasti jatkaa taikaneliöiden sisältämän matematiikan pariin.

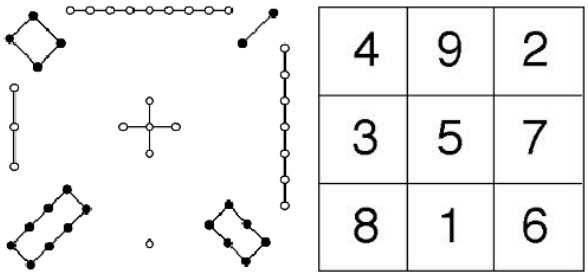
Taikaneliöitä ei enää nykypäivänä pidetä yliluonnollisia ominaisuuksia sisältävinä mystisinä asioina, vaan niillä on ihmisten keskuudessa enää lähinnä viihteellinen merkitys. Tässä tutkielmassa rajoitutaan kertaluvun p taikaneliöihin, missä p on alkuluku. Luvussa kolme tarkastellaan ensin tavallisia taikaneliötä, jonka jälkeen siirrytään lineaaristen taikaneliöiden käsittelyyn. Neljännessä luvussa esitellään menetelmä, jota voidaan hyödyntää kertaluvun p lineaaristen taikaneliöiden laadinnassa, sekä samalla perehdytään kertaluvun p lineaaristen taikaneliöiden olemassaoloon. Tutkielman päälähteenä on käytetty John Lorchin artikkelia Magic Squares and Sudoku, joka on julkaistu The American Mathematical Monthly -lehden marraskuun numerossa vuonna 2012.

Sisältö

1 Johdanto

Taikaneliö on $n \times n$-neliö ($n \in \mathbb{Z}_+$), joka sisältää joukon numeroita, tavallisesti $\{1, 2, \ldots, n^2\}$ siten, että jokaisen rivin, sarakkeen ja molempien lävistäjien sisältämät luvut summautuvat samaksi luvuksi. Tällaiset neliöt ovat kiehtoneet niin matemaatikkoja, kuin muitakin ihmisiä jo monien vuosisatojen ajan. Niiden alkuperästä ja syntyhistoriasta ei tiedetä juurikaan mitään. Monet näkemykset asiasta ovat ristiriitaisia ja jopa liioiteltuja, joten varmaa tai yksikäsitteistä historiakatsausta on vaikea löytää. Seuraavissa kappaleissa esitellään taikaneliöiden historiaa lähdeteosten Before Sudoku, The World of Magic Squares [1] ja The Zen of Magic Squares, Circles and Stars [4] avulla.

Nykytietojen mukaan Kiina, Intia ja arabimaat ovat olleet vahvasti mukana taikaneliöiden luomisessa. Kaikille näille kulttuureille yhteistä on se, että taikaneliöiden on ajateltu pitävän sisällään yliluonnollisia ominaisuuksia. Nimitys *taikaneliö* sopii myös hyvin yhteen niiden käyttötarkoitukseen antiikissa ja keskiajalla, jolloin taikaneliöitä kaiverrettiin talismaaneihin ja amuletteihin tuomaan onnea ja suojelemaan pahalta. Uskonnollisten ja suojelusymbolien lisäksi taikaneliöitä on käytetty muun muassa tulevaisuuden ennustamisen välineenä ja tähtitieteen maailmassa. Kun taikaneliöt myöhemmin menettivät mystiset merkityksensä, ne jäivät kuitenkin pysyvästi ihmisten keskuuteen. Matemaatikot jatkoivat niiden tarkastelua lukuteoreettiselta kannalta ja muut ihmiset ottivat ne lähinnä viihteelliseen käyttöön.

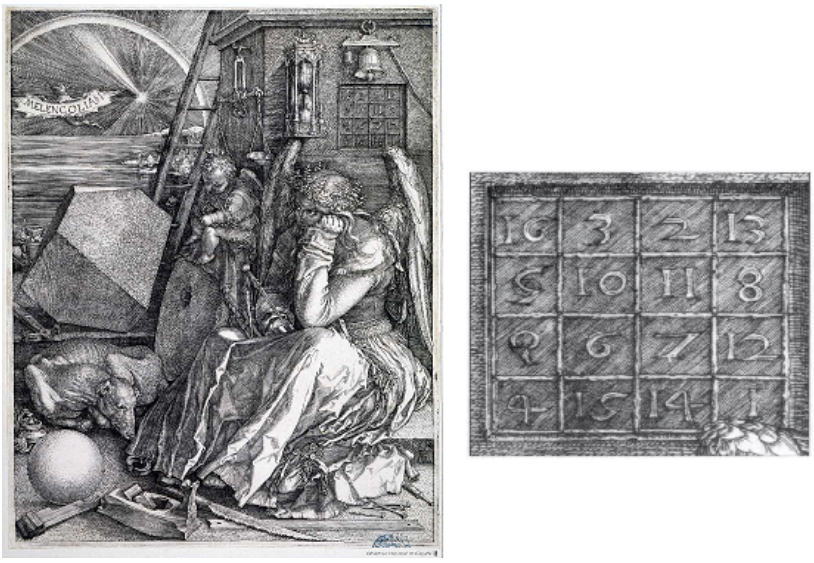


Kuva 1. Lo Shu -taikaneliö. Vasemmanpuoleisessa kuvassa hahmotelma kilpikonnan kilpikuvioinnista ja oikealla moderni esitys samasta asiasta.

Vanhin tunnettu taikaneliö ajoittuu monen tuhannen vuoden takaiseen Kiinaan. Erään tarinan mukaan tuolloin muinaisessa Kiinassa ihmisten riesana olivat valtavat tulvat, jotka tuhosivat viljelyksiä ja asuinmaata. Ihmiset kokivat tulvat joen jumalien vihana ja yrittivät hillitä tätä vihaa antamalla uhrilahjoja. Yksi tulvivista joista oli nimeltään *Lo*-joki, jonka jumalaa ihmiset yrittivät uhrilahjoin lepyttää. Joka kerta uhrauksen jälkeen joesta nousi suuri kilpikonna, joka liikkui uhrilahjan ympärillä palaten kuitenkin aina takaisin jokeen. Tulvat jatkuivat ja näytti siltä, että joen jumala ei hyväksynyt uhrausta. Eräänä päivänä joku ihmisistä kiinnitti huomion kilpikonnan kilvessä olevaan ainutlaatuiseen kuviointiin. Kilvessä esiintyi pieniä pisteryppäitä, joista muodostui kokonaisluvut yhdestä yhdeksään. Pisteryppäät olivat

asettuneet 3×3-ruudukon muotoon, jonka rivien, sarakkeiden ja lävistäjien summaksi tuli 15. Tämä havainto auttoi ihmisiä selviytymään tulvivan joen kanssa. Yhden tarinan mukaan tulviva joki saatiin aisoihin 15 uhrilahjan turvin, toinen tarina kertoo luvun 15 liittyvän Kiinan aurinkokalenteriin, joka toimi ihmisille apukeinona. Tämä taikaneliö tunnetaan *Lo Shu*-neliönä, ja on vanhin tiedossamme oleva 3×3 eli kertaluvun kolme taikaneliö.

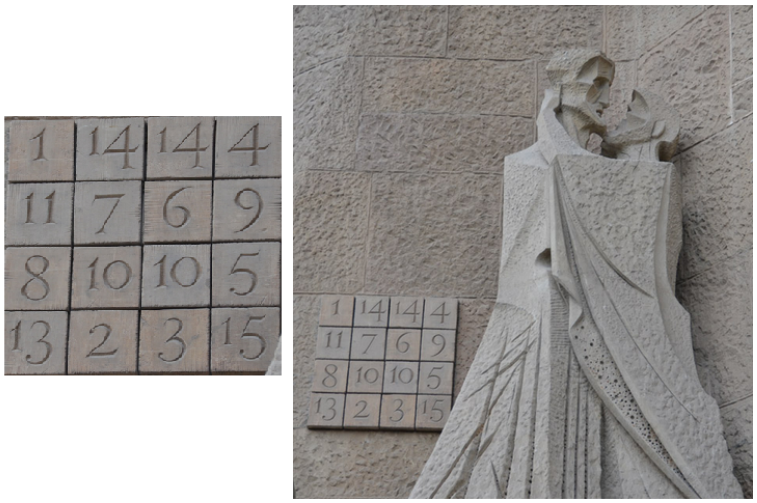
Todennäköisimmin taikaneliöt kulkeutuivat Kiinasta Intian kautta arabimaihin ja sieltä Eurooppaan. Vanhimmat taikaneliöhavainnot Intiasta ovat ensimmäiseltä ja arabimaista kahdeksannelta vuosisadalta, kunnes tiettävästi 1300-luvun tietämillä Manual Moschopouloksen johdolla taikaneliöt rantautuivat Eurooppaan. Ensimmäiset todisteet taikaneliöiden esiintymisestä länsimaissa paljastui kuuluisan saksalaisen taidemaalarin Albrecht Dürerin kaiverruksesta. Hänen vuonna 1514 tekemän kuparikaiverrustyön *Melankolia 1* oikeaan yläkulmaan on sisällytetty 4×4-taikaneliö. Kaiverruksessa esiintyvä *Dürerin neliö* on yksi tunnetuimpia eurooppalaisia taikaneliöitä.



Kuva 2. Vasemmalla Albrecht Dürerin Melankolia 1 -taideteos ja oikealla Dürerin neliö.

Taikaneliöiden laatimissääntöihin alettiin ottaa vapauksia 1900-luvun tienoilla, ja nämä vapaammat säännöt ovat mahdollistaneet uudenlaisten taikaneliövariaatioiden synnyn. Tätä ennen taikaneliöt laadittiin pitkälti käyttäen peräkkäisiä kokonaislukuja luvusta yksi eteenpäin siten, että mikään luku ei toistu neliössä kahta kertaa. Uudet säännökset mahdollistivat esimerkiksi nollan sijoittamisen taikaneliön alkioksi, samoin kuin lukujen toistuvuus tai pois jättäminen oli nyt mahdollista. Yksi tällainen vapaamman menetelmän taikaneliö on espanjalaisen kuvanveistäjä Josep Subirachin suunnittelema taikaneliö, joka tunnetaan *Sagrada Familia* -taikaneliönä. Se sijaitsee Sagrada Familia -katedraalin julkisivulla Barcelonassa Espanjassa. Kyseessä on Dürerin taikaneliön tapaan 4×4-taikaneliö, joka alkaa luvusta yksi, mut-

ta sisältää luvut 10 ja 14 kaksi kertaa, sekä luvut 12 ja 16 puuttuvat. Tämän neliön rivien, sarakkeiden ja lävistäjien luvut summautuvat luvuksi 33, jota pidetään Jeesuksen kuolinikänä.



Kuva 3. Sagrada Familia -taikaneliö.

On syytä huomata, että edellä esitetyt 4×4-taikaneliöt tuottavat keskenään erisuuruiset rivi-, sarake-, ja diagonaalisummat. Dürerin neliössä nämä alkiot summautuvat luvuksi 34, ja Sagrada Familia -neliössä kyseinen summa on 33. Tämä johtuu puhtaasti siitä, että nämä taikaneliöt on laadittu eri laatimissäännöillä. Yhtenevin säännöin laaditut saman kertaluvun taikaneliöt tuottavat aina yhtä suuret rivi-, sarake- ja diagonaalisummat.

Kuten jo edellä on todettu, nykyisin taikaneliöillä ei ole enää yliluonnollisia tai mystisiä merkityksiä, vaan niiden rooli ihmisten keskuudessa on lähinnä viihteellinen. Tässä tutkielmassa tutustutaan lineaarisiin taikaneliöihin ja katsotaan, millaisella menetelmällä niitä on mahdollista konstruoida suhteellisen yksinkertaisesti. Tutkielmassa rajoitutaan kertaluvun p taikaneliöihin, missä p on alkuluku, ja taikaneliöön sijoitetaan kokonaislukuja nollasta alkaen. Tutkielman päälähteenä on käytetty John Lorchin artikkelia Magic Squares and Sudoku [3], joka on julkaistu The American Mathematical Monthly -lehden marraskuun numerossa vuonna 2012. Artikkelista käsitellään sivujen 759-765 sisältö. Luvussa kaksi on käsitelty kertauksenomaisesti keskeisimmät matemaattiset sisällöt, jotka lukijan on hallittava ymmärtääkseen tutkielman myöhempää sisältöä. Luku kolme keskittyy lineaarisiin taikaneliöihin, josta jatketaan lukuun neljä, missä perehdytään lineaaristen taikaneliöiden konstruointiin ja olemassaoloon.

2 Herättelyä matemaattiseen ajatteluun

Tässä luvussa käsitellään kertauksenomaisesti keskeisimmät matemaattiset sisällöt, jotka lukijan on hallittava ymmärtääkseen tutkielman myöhempää sisältöä. Ensin käsitellään äärellisiä kuntia, jonka jälkeen siirrytään vektoriavaruuksiin ja aliavaruuksiin. Lopuksi käsitellään jakoyhtälöitä ja lukujärjestelmiä. Tässä luvussa useimmat todistukset tullaan sivuuttamaan.

2.1 Äärellisistä kunnista

Tässä aliluvussa kerrataan, mitä äärellisellä kunnalla tarkoitetaan. Määritelmät ja lauseet pohjautuvat Marko Rinta-ahon Oulun yliopistossa luennoimaan Äärelliset kunnat -kurssin luentomateriaaliin vuodelta 2011 [5].

Määritelmä 2.1. Kommutatiivinen rengas $R \neq \{0\}$ on *kunta*, mikäli jokainen nollasta eroava alkio on kääntyvä, eli jokaisella $0 \neq x \in R$ on käänteisalkio $x^{-1} \in R$.

Esimerkki 2.2. $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia.

Esimerkki 2.3. Kokonaislukujen joukko $\mathbb{Z}$ ei muodosta kuntaa, sillä esimerkiksi alkiolla 5 ei ole käänteisalkiota joukossa $\mathbb{Z}$.

Lause 2.4. *$\mathbb{Z}_n$ on kunta, jos ja vain jos n on alkuluku.* □

Määritelmä 2.5. Olkoon K kunta. Pienintä positiivista kokonaislukua n, jolle pätee

$$\underbrace{1 + \cdots + 1}_{n \text{ kpl}} = 0,$$

kutsutaan K:n *karakteristikaksi* ja merkitään $\operatorname{char} K$.

Lause 2.6. *Kunnan karakteristika on aina* 0 *tai alkuluku.* □

Määritelmä 2.7. *Äärellinen kunta* on kunta, jonka alkioiden lukumäärä on äärellinen.

Merkintä 2.8. Äärelliselle kunnalle $\mathbb{F}$, jonka kertaluku on q, käytetään merkintää $\mathbb{F}_q$.

Esimerkki 2.9. Yksinkertaisin esimerkki äärellisestä kunnasta on binäärikunta $\mathbb{F}_2 = (\mathbb{Z}_2, +, \cdot)$.

Esimerkki 2.10. Jäännösluokkarengas $(\mathbb{Z}_p, +, \cdot)$ muodostaa kunnan, jossa on p alkiota. Toisin sanoen $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.

Määritelmä 2.11. Äärellisen kunnan *kertaluvulla* tarkoitetaan kunnan alkioiden lukumäärää.

Esimerkki 2.12. Äärellisen kunnan $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ kertaluku on p.

Äärellisen kunnan rakenne on määrätty tarkoin. Seuraavassa lausesssa annetaan rajoitus äärellisen kunnan alkioiden lukumäärälle.

Lause 2.13. *Äärellisen kunnan $\mathbb{F}$ kertaluku on muotoa p^k, missä $k \in \mathbb{Z}_+$ ja $p = char\, \mathbb{F}$.* $\square$

Esimerkki 2.14. Äärellisen kunnan $\mathbb{F}_4$ kertaluku on 4 ja char $\mathbb{F}_4 = 2$.

Taikaneliön rivit ja sarakkeet indeksöidään äärellisen kunnan $\mathbb{F}$ alkioiksi siten, että rivien ja sarakkeiden numerointi alkaa kunnan pienimmän alkion mukaan kasvavassa järjestyksessä ylhäältä alas, ja vasemmalta oikealle mentäessä. Näin ollen, kun jatkossa taikaneliöiden yhteydessä käsittelemme kuntaa $\mathbb{Z}_p$, rivit ja sarakkeet ovat joukon $\{0, 1, \ldots, p-1\}$ alkioita. Samoin alkion paikka taikaneliössä voidaan ilmaista koordinaattina $(x, y) \in \mathbb{F}^2$, missä x ilmaisee rivin ja y sarakkeen.

Huomautus 2.15. Taikaneliö voidaan ajatella matriisin kaltaisena rakenteena, jolle ei kuitenkaan määritellä laskutoimituksia, tai jota ei operoida kuten matriisia. Rivien ja sarakkeiden indeksöinnissä käytetään tavanomaista matriisien indeksöintitapaa.

Esimerkki 2.16. Johdannossa esiintyneessä Lo Shu -neliössä (Kuva 1)

(a) rivi 2 sisältää alkiot $8, 1, 6$

(b) sarake 0 sisältää alkiot $4, 3, 8$

(c) luku 9 sijaitsee paikassa $(0, 1)$.

2.2 Vektoriavaruuksista, aliavaruuksista ja kannoista

Tässä aliluvussa määritellään vektoriavaruus, aliavaruus ja vektoriavaruuden kanta. Määritelmät pohjautuvat Joseph J. Rotmanin kirjaan Advanced Modern Algebra [6]. Teorian tueksi on esitetty myös muutama helpohko esimerkkitehtävä.

2.2.1 Vektoriavaruus

Määritelmä 2.17. Olkoon V epätyhjä joukko, K äärellinen kunta ja joukko V varustettu laskutoimituksilla $+ : V \times V \to V$ (yhteenlasku) ja $\cdot : K \times V \to V$ (skalaarilla kertominen). Tällöin kolmikkoa $(V, +, \cdot)$ sanotaan *K-vektoriavaruudeksi V*, jos

1. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ kaikilla $\mathbf{u}, \mathbf{v} \in V$

2. $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ kaikilla $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$

3. yhteenlaskulla on neutraalialkio $\mathbf{0}$, jolle kaikilla $\mathbf{u} \in V$ pätee $\mathbf{u} + \mathbf{0} = \mathbf{u}$
4. kaikille $\mathbf{u} \in V$ on olemassa vastavektori $-\mathbf{u} \in V$ siten, että $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$
5. $k(\mathbf{u} + \mathbf{v}) = k\mathbf{u} + k\mathbf{v}$ kun $\mathbf{u}, \mathbf{v} \in V$ ja $k \in K$
6. $(k + l)\mathbf{u} = k\mathbf{u} + l\mathbf{u}$ kaikilla $\mathbf{u} \in V$ ja $k, l \in K$
7. $k(l\mathbf{u}) = (kl)\mathbf{u}$ kaikilla $\mathbf{u} \in V$ ja $k, l \in K$
8. $1\mathbf{u} = \mathbf{u}$ kaikilla $\mathbf{u} \in V$.

Joukon V alkioita sanotaan *vektoreiksi* ja kunnan K alkioita *skalaareiksi*.

Esimerkki 2.18. Olkoon $K^n = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) \mid x_i \in K\}$, missä K on äärellinen kunta ja $n \in \mathbb{N}$. Olkoot $\mathbf{x}, \mathbf{y} \in K^n$ ja $k, l \in K$ ja määritellään yhteenlasku ja skalaarilla kertominen siten, että

$$\mathbf{x} + \mathbf{y} = (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

ja

$$k\mathbf{x} = k(x_1, x_2, \ldots, x_n) = (kx_1, kx_2, \ldots, kx_n).$$

Tällöin kunnan K ominaisuuksista seuraa, että K^n on K-kertoiminen vektoriavaruus, sillä se toteuttaa vektoriavaruuden aksioomat.

2.2.2 Aliavaruus

Määritelmä 2.19. Olkoon V vektoriavaruus ja $W \subseteq V$ epätyhjä. Jos W on vektoriavaruus avaruuden V operaatioiden suhteen, W on avaruuden V *aliavaruus*.

Lause 2.20. *(Aliavaruuskriteeri) Vektoriavaruuden V epätyhjä osajoukko W muodostaa aliavaruuden, jos ja vain jos*

1. $\mathbf{u} + \mathbf{v} \in W$
2. $k\mathbf{u} \in W$

aina, kun $\mathbf{u}, \mathbf{v} \in W$ ja $k \in K$. □

Esimerkki 2.21. Olkoon $W = \{(k, 3k) \mid k \in \mathbb{R}\}$. Nyt W on avaruuden $\mathbb{R}^2$ alivaruus lauseen 2.20 nojalla, sillä

1. $(l, 3l) + (m, 3m) = (l + m, 3l + 3m) = (l + m, 3(l + m)) \in W$
2. $n(l, 3l) = (nl, n(3l)) = (nl, 3(nl)) \in W$,

kun $(l, 3l), (m, 3m) \in W$ ja $n \in \mathbb{R}$.

Esimerkki 2.22. Vektoriavaruus $W = \{(2k, 3k + 1) \mid k \in \mathbb{R}\}$ ei ole avaruuden $\mathbb{R}^2$ aliavaruus. Tämä voidaan todeta osoittamalla, että origo $\mathbf{0} = (0, 0)$ ei kuulu joukkoon W. Tarkastellaan esimerkiksi vektoria $(2l, 3l + 1) \in W$. Nyt, jos $l = 0$, niin $3l + 1 = 1 \neq 0$, jolloin $\mathbf{0} = (0, 0) \notin W$. Näin ollen W ei ole aliavaruus.

2.2.3 Kanta ja dimensio

Määritelmä 2.23. Olkoon $S = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}\} \subseteq V$. Merkitään $\mathrm{Lin}(S) = \{k_1\mathbf{v_1} + k_2\mathbf{v_2} + \cdots + k_n\mathbf{v_n} \mid k_1, k_2, \ldots, k_n \in K\}$. Vektorit, jotka kuuluvat $\mathrm{Lin}(S)$:ään, ovat joukon S vektorien *lineaarikombinaatioita*.

Määritelmä 2.24. Lineaarikombinaatioiden joukkoa eli $\mathrm{Lin}(S)$:ää sanotaan joukon S *virittämäksi aliavaruudeksi*.

Merkintä 2.25. Joukon S virittämälle aliavaruudelle käytetään $\mathrm{Lin}(S)$:n lisäksi myös merkintää $\langle S \rangle$.

Huomautus 2.26. Aliavaruuden määritelmästä 2.19 seuraa, että $\mathrm{Lin}(S)$ on joukon S aliavaruus.

Määritelmä 2.27. Olkoon $S = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}\} \subseteq V$. Joukko S on *vapaa*, mikäli seuraava ehto on voimassa: jos

$$\sum_{i=1}^{n} k_i\mathbf{v}_i = \mathbf{0},$$

niin

$$k_1 = k_2 = \cdots = k_n = 0.$$

Muulloin S on *sidottu*.

Määritelmä 2.28. Olkoon $S = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}\} \subseteq V$. Joukko S on vektoriavaruuden V *kanta*, mikäli S on vapaa ja virittää V:n.

Määritelmä 2.29. Olkoon vektoriavaruudella V kanta S, missä $|S| = n < \infty$. Kannan alkioiden lukumäärää n sanotaan vektoriavaruuden V *dimensioksi* ja sitä merkitään $\dim V = n$. Sanotaan myös, että V on *n-ulotteinen*.

Määritelmä 2.30. Jos vektoriavaruudella $V \neq \emptyset$ on äärellinen kanta, V on *äärellisulotteinen*. Muussa tapauksessa vektoriavaruuden dimensio on ääretön.

Lause 2.31. *Jokaisella vektoriavaruudella $V \neq \{0\}$ on kanta. Jos V on äärellisulotteinen, niin jokaisessa kannassa on yhtä monta alkiota.* □

Edellisen lauseen tuloksesta seuraa, että vektoriavaruuden V dimensio on hyvinmääritelty.

Esimerkki 2.32. Olkoon V vektoriavaruus ja W sen aliavaruus. Oletetaan, että aliavaruuden W kanta on $\{\mathbf{x}\}$, $\mathbf{x} \neq \mathbf{0}$. Koska $\dim W = 1$, sanotaan, että W on yksiulotteinen.

Esimerkki 2.33. Jos aliavaruuden W kanta on $\emptyset$, niin W on nolla-avaruus.

Esimerkki 2.34. Tarkastellaan seuraavaksi 5×5-ruudukkoa, jonka rivit ja sarakkeet indeksöidään äärellisen kunnan $\mathbb{Z}_5$ alkioiksi aliluvussa 2.1 esitetyllä tavalla. Nyt pisteen $(1,1)$ virittämä yksiulotteinen aliavaruus on

$$\langle (1,1) \rangle = \{r(1,1) \mid r \in \mathbb{F}\} = \{(r,r) \mid r \in \mathbb{F}\} = \{(0,0),(1,1),(2,2),(3,3),(4,4)\},$$

jolloin aliavaruuden $\langle (1,1) \rangle$ toisistaan erilliset sivuluokat ovat

$$\begin{aligned}
(0,0) + \langle (1,1) \rangle &= \{(0,0),(1,1),(2,2),(3,3),(4,4)\} \\
(0,1) + \langle (1,1) \rangle &= \{(0,1),(1,2),(2,3),(3,4),(4,0)\} \\
(0,2) + \langle (1,1) \rangle &= \{(0,2),(1,3),(2,4),(3,0),(4,1)\} \\
(0,3) + \langle (1,1) \rangle &= \{(0,3),(1,4),(2,0),(3,1),(4,2)\} \\
(0,4) + \langle (1,1) \rangle &= \{(0,4),(1,0),(2,1),(3,2),(4,3)\}.
\end{aligned}$$

Seuraavaksi on esitetty näistä kolmen ensimmäisen sivuluokan sisältämät pisteet 5×5-ruudukossa niin, että kirjain X kuvastaa aina sivuluokan yhtä pistettä.

X	o	o	o	o
o	X	o	o	o
o	o	X	o	o
o	o	o	X	o
o	o	o	o	X

o	X	o	o	o
o	o	X	o	o
o	o	o	X	o
o	o	o	o	X
X	o	o	o	o

o	o	X	o	o
o	o	o	X	o
o	o	o	o	X
X	o	o	o	o
o	X	o	o	o

Pisteen $(1,4)$ virittämä yksiulotteinen aliavaruus $\langle (1,4) \rangle$ puolestaan on

$$\langle (1,4) \rangle = \{r(1,4) \mid r \in \mathbb{F}\} = \{(0,0),(1,4),(2,3),(3,2),(4,1)\},$$

ja aliavaruuden $\langle (1,4) \rangle$ toisistaan erilliset sivuluokat ovat

$$\begin{aligned}
(0,0) + \langle (1,4) \rangle &= \{(0,0),(1,4),(2,3),(3,2),(4,1)\} \\
(0,1) + \langle (1,4) \rangle &= \{(0,1),(1,0),(2,4),(3,3),(4,2)\} \\
(0,2) + \langle (1,4) \rangle &= \{(0,2),(1,1),(2,0),(3,4),(4,3)\} \\
(0,3) + \langle (1,4) \rangle &= \{(0,3),(1,2),(2,1),(3,0),(4,4)\} \\
(0,4) + \langle (1,4) \rangle &= \{(0,4),(1,3),(2,2),(3,1),(4,0)\}.
\end{aligned}$$

Alla on esitetty jälleen näistä kolmen ensimmäisen sivuluokan pisteet ruudukkoon sijoitettuna.

X	o	o	o	o
o	o	o	o	X
o	o	o	X	o
o	o	X	o	o
o	X	o	o	o

o	X	o	o	o
X	o	o	o	o
o	o	o	o	X
o	o	o	X	o
o	o	X	o	o

o	o	X	o	o
o	X	o	o	o
X	o	o	o	o
o	o	o	o	X
o	o	o	X	o

2.3 Lukujärjestelmistä

Yleisesti on totuttu siihen, että luvut esitetään kymmenjärjestelmässä, eli luku esitetään kantaluvun 10 potenssisummana. Kantaluvuksi voidaan kuitenkin valita jokin muu nollasta eroava luonnollinen luku n, jolloin lukujärjestelmä vaihtuu n-järjestelmäksi. Kokonaislukujen jakoyhtälöt helpottavat lukumuunnoksia lukujärjestelmien välillä, joten aloitetaan aliluku jakoyhtälöiden käsittelyllä. Tämän aliluvun sisältö pohjautuu Joseph J. Rotmanin kirjaan A First Course in Abstract Algebra [7] sekä lauseen 2.37 todistuksessa on hyödynnetty Eero Hyryn Tampereen yliopistossa luennoiman Algebra 1 -kurssin luentomuistiinpanoja [2].

Määritelmä 2.35. Olkoon $0 \neq d \in \mathbb{N}$, $x, q, r \in \mathbb{Z}$ ja $0 \leq r < d$. Tällöin yhtälöä $x = qd + r$ sanotaan *jakoyhtälöksi*.

Määritelmä 2.36. Jakoyhtälön luku x on *jaettava*, d *jakaja*, q *osamäärä* ja luku r on *jakojäännös*.

Lause 2.37. *Olkoon* $0 \neq d \in \mathbb{N}$. *Jos* $x \in \mathbb{Z}$, *niin on olemassa yksikäsitteiset* $q, r \in \mathbb{Z}$ *siten, että* $x = qd + r$ *ja* $0 \leq r < d$.

Todistus. Osoitetaan ensin olemassaolo. Tarkastellaan joukkoa

$$M := \{x - qd \mid q \in \mathbb{Z}\} \cap \mathbb{N}.$$

Pitää osoittaa, että $M \neq \emptyset$, eli että on olemassa $q \in \mathbb{Z}$ siten, että $x - qd \geq 0$. Jos $x \geq 0$, niin $q = 0$ kelpaa. Jos taas $x < 0$, niin valitaan $q = x$, jolloin

$$x - qd = x - xd = x(1 - d) \geq 0.$$

Täten $\mathbb{N}$ on hyvin järjestetty, joten joukossa M on pienin luku r. Nyt $r \in M$, joten jollakin $q \in \mathbb{Z}$ pätee $r = x - qd$ eli $x = qd + r$. Ja koska jos $r \in M$, niin $r \geq 0$.

On vielä osoitettava, että $r < d$. Tehdään vastaoletus $r \geq d$. Jos nyt $r \geq d$, niin $r - d \geq 0$ ja $r - d = (x - qd) - d = x - (q + 1)d$. Siis $r - d \in M$. Tämä johtaa kuitenkin ristiriitaan, sillä nyt $r - d < r$ ja r oli joukon M pienin luku. Näin ollen oltava $r < d$.

Osoitetaan vielä, että jakoyhtälön esitys on yksikäsitteinen. Oletetaan, että

$$x = q_1 d + r_1 = q_2 d + r_2, \text{ missä } 0 \leq r_1 < d \text{ ja } 0 \leq r_2 < d.$$

Tehdään lisäoletus, että $r_1 \leq r_2$. Tällöin

$$r_2 - r_1 = x - q_2 d - (x - q_1 d) = (q_1 - q_2)d.$$

Nyt koska $0 \leq r_2 - r_1 \leq r_2 < d$, niin $0 \leq (q_1 - q_2)d < d$. Tästä seuraa, että $0 \leq q_1 - q_2 < 1$. Koska $q_1, q_2 \in \mathbb{Z}$, niin on oltava, että $q_1 = q_2$. Näin ollen $r_2 - r_1 = (q_1 - q_2)d = 0$, joten $r_2 = r_1$. [2] □

Jakoyhtälön yksikäsitteisyydestä seuraa, että jokainen luonnollinen luku $n \in \mathbb{N}$ on mahdollista esittää yksikäsitteisenä potenssisummana valitun kantaluvun avulla niin, että

$$n = x_k d^k + x_{k-1} d^{k-1} + \cdots + x_1 d + x_0 =: (x_k, \ldots, x_1, x_0)_d,$$

missä $k \geq 0$ ja $x_i \in \{0, \ldots, d-1\}$ kaikilla $i = 0, \ldots, k$. Kyseinen potenssisumma saadaan muodostettua jakoyhtälön avulla toistamalla luvulla d jakamista useamman kerran peräkkäin. Mikäli kantaluku $d \neq 10$, se merkitään alaindeksinä näkyviin, tai osoitetaan muulla tavoin mitä kantalukua on käytetty (vrt. esimerkki 2.38).

Esimerkki 2.38. Vaihdetaan Dürerin neliön alkiot vastaamaan tässä tutkielmassa käytettyjä merkintöjä, joten vähennetään jokaisesta ruudusta yksi. Nyt neliö sisältää alkiot $\lambda \in \{0, 1, \ldots, 15\}$. Nämä kokonaisluvut voidaan esittää 4-järjestelmässä siten, että

$$\lambda = \lambda_4 \cdot 4^1 + \lambda_1 \cdot 4^0 = \lambda_4 \cdot 4 + \lambda_1 \cdot 1,$$

missä $\lambda_4 = \lfloor \lambda/4 \rfloor$ ja λ_1 on jakoyhtälön jakojäännös. Kokonaisluku λ voidaan esittää 4-järjestelmässä myös niin, että $\lambda = (\lambda_4, \lambda_1)$. Dürerin neliö 4-järjestelmässä kirjoitettuna on esitetty alla.

(3,3)	(0,2)	(0,1)	(3,0)
(1,0)	(2,1)	(2,2)	(1,3)
(2,0)	(1,1)	(1,2)	(2,3)
(0,3)	(3,2)	(3,1)	(0,0)

3 Lineaariset taikaneliöt

Perinteisesti taikaneliöt on laadittu käyttäen peräkkäisiä kokonaislukuja luvusta yksi eteenpäin siten, että mikään luku ei toistu neliössä kahta kertaa. Mutta kuten aiemmin on jo ollut esillä, taikaneliöiden laadinta on myös mahdollista erilaisin variaatioin. Tässä tutkielmassa taikaneliöön sijoitetaan peräkkäiset kokonaisluvut nollasta eteenpäin niin, että sama luku ei esiinny taikaneliön alkiona kuin kerran.

Tässä luvussa määritellään ensin taikaneliö ja taikasumma, jonka jälkeen siirrytään lineaarisiin taikaneliöihin, joita käsitellään alaluvussa 3.2. Tästä eteenpäin tutkielman taustalla olevana lähdekirjallisuutena on käytetty John Lorchin artikkelia Magic Squares and Sudoku [3]. Artikkelin sisältöä on täydennetty niin teorian kuin esimerkkitehtävienkin osalta.

3.1 Taikaneliö

Määritelmä 3.1. *Taikaneliöksi* kutsutaan $q \times q$-ruudukkoa, $q > 1$, jonka ruudut täytetään toisistaan eriävillä kokonaisluvuilla $\{0, 1, \ldots, q^2 - 1\}$ niin, että ruutujen sisältämien lukujen summa on sama jokaisella rivillä, sarakkeella ja lävistäjällä.

Määritelmä 3.2. *Kertaluvun* q taikaneliöksi sanotaan $q \times q$-taikaneliötä, missä $q \in \mathbb{N}$.

Esimerkki 3.3. Pienin ei-triviaali taikaneliö on kertaluvun kolme taikaneliö, sillä kertaluvun kaksi taikaneliötä ei ole olemassa. Osoitetaan seuraavaksi konstruoimalla, että kertaluvun kaksi taikaneliö ei tosiaankaan ole mahdollinen.

Oletetaan, että kertaluvun kaksi taikaneliö olisi olemassa ja sisältää toisistaan eriävät kokonaisluvut $a, b, c, d \in \{0, 1, 2, 3\}$ kuten alla on esitetty.

a	b
c	d

Nyt, koska taikaneliön määritelmän mukaan jokaisen rivin, sarakkeen ja lävistäjän sisältämien alkioiden täytyy summautua samaksi luvuksi, voidaan kirjoittaa, että $a + b = a + c$. Tästä seuraa selvästi, että $b = c$, mikä johtaa ristiriitaan oletuksen kanssa. Näin ollen, kertaluvun kaksi taikaneliötä ei ole olemassa.

Kertaluvun kolme taikaneliö saadaan muodostettua esimerkiksi johdannossa esiintyneestä Lo Shu -neliöstä (Kuva 1) vähentämällä jokaisen ruudun alkiosta yksi.

Kertaluvun q taikaneliön alkioiden summasta saadaan q^2:n alkion muodostama aritmeettinen sarja

$$0 + 1 + 2 + \cdots + q^2 - 1 = \frac{q^2(0 + (q^2 - 1))}{2} = \frac{q^2(q^2 - 1)}{2}.$$

Jakamalla tämä taikaneliön alkioiden summa rivien ja sarakkeiden lukumäärällä q, saadaan

$$\frac{q(q^2 - 1)}{2},$$

joka on yhden rivin, sarakkeen ja lävistäjän sisältämien lukujen summa.

Määritelmä 3.4. Kertalukua q olevan taikaneliön rivien, sarakkeiden ja lävistäjien sisältämät luvut summautuvat luvuksi $q(q^2 - 1)/2$. Tätä lukua kutsutaan *taikasummaksi*.

Esimerkki 3.5. Seuraava ruudukko on kertaluvun viisi taikaneliö, jonka taikasumma on 60, sillä jokaisen rivin, sarakkeen ja lävistäjän sisältämät alkiot summautuvat luvuksi 60. Esimerkissä 4.4 käydään läpi vaihtoehtoinen tapa osoittaa rivien, sarakkeiden ja lävistäjien sisältämien lukujen summa samaksi.

0	23	16	14	7
19	12	5	3	21
8	1	24	17	10
22	15	13	6	4
11	9	2	20	18

Tämä taikaneliö toimii pääesimerkkinä tutkielman myöhemmässä vaiheessa ja siihen palataan useaan otteeseen.

Esimerkki 3.6. Tämä ruudukko ei ole taikaneliö. Miksi?

0	7	14	16	**23**
17	24	1	**8**	10
9	11	**18**	20	2
21	**3**	5	12	19
13	15	22	4	6

Ruudukko ei toteuta taikaneliön määritelmää, sillä sivulävistäjän alkiot eivät summaudu taikasummaksi. Rivi- ja sarakesummat, sekä päädiagonaalin alkioiden summa täyttää kuitenkin taikaneliön ehdot.

3.2 Lineaarinen taikaneliö

Määritelmä 3.7. Kertaluvun q taikaneliö, joka sisältää kokonaisluvut $\{0, 1, \ldots, q^2 - 1\}$, on *lineaarinen taikaneliö*, jos

(i) jokaisen rivin ja sarakkeen summa on $q(q^2 - 1)/2$

(ii) jokaisen yksiulotteisen aliavaruuden $\langle(1, 1)\rangle \in \mathbb{F}^2$ sivuluokan sisältämien lukujen summa on $q(q^2 - 1)/2$

(iii) jokaisen yksiulotteisen aliavaruuden $\langle(1, -1)\rangle \in \mathbb{F}^2$ sivuluokan sisältämien lukujen summa on $q(q^2 - 1)/2$.

Esimerkki 3.8. Osoitetaan, että esimerkin 3.5 taikaneliö on lineaarinen taikaneliö.

0	23	16	14	7
19	12	5	3	21
8	1	24	17	10
22	15	13	6	4
11	9	2	20	18

(i) Tämä on todettu esimerkissä 3.5.

(ii) Pisteen (1,1) virittämän yksiulotteisen aliavaruuden $\langle(1, 1)\rangle$ toisistaan erilliset sivuluokat on käsitelty esimerkissä 2.34.

Näiden sivuluokkien sisältämien lukujen summat tarkasteltavassa taikaneliössä ovat

$$\begin{aligned}
(0, 0) + \langle(1, 1)\rangle &: 0 + 12 + 24 + 6 + 18 = 60 \\
(0, 1) + \langle(1, 1)\rangle &: 23 + 5 + 17 + 4 + 11 = 60 \\
(0, 2) + \langle(1, 1)\rangle &: 16 + 3 + 10 + 22 + 9 = 60 \\
(0, 3) + \langle(1, 1)\rangle &: 14 + 21 + 8 + 15 + 2 = 60 \\
(0, 4) + \langle(1, 1)\rangle &: 7 + 19 + 1 + 13 + 20 = 60.
\end{aligned}$$

(iii) Pisteen $(1, -1)$ virittämän yksiulotteisen aliavaruuden $\langle(1, -1)\rangle$ toisistaan erilliset sivuluokat on niin ikään käsitelty esimerkissä 2.34, sillä $-1 \equiv 4 \pmod 5$, jolloin $\langle(1, -1)\rangle = \langle(1, 4)\rangle$.

Näiden sivuluokkien sisältämien lukujen summat tarkasteltavassa taikaneliössä ovat

$$(0,0) + \langle(1,4)\rangle : 0 + 21 + 17 + 13 + 9 = 60$$
$$(0,1) + \langle(1,4)\rangle : 23 + 19 + 10 + 6 + 2 = 60$$
$$(0,2) + \langle(1,4)\rangle : 16 + 12 + 8 + 4 + 20 = 60$$
$$(0,3) + \langle(1,4)\rangle : 14 + 5 + 1 + 22 + 18 = 60$$
$$(0,4) + \langle(1,4)\rangle : 7 + 3 + 24 + 15 + 11 = 60.$$

On osoitettu, että määritelmän 3.7 kohdat (i)-(iii) toteutuvat, joten esimerkin 3.5 taikaneliö on lineaarinen taikaneliö.

Esimerkki 3.9. Tämä taikaneliö ei ole lineaarinen taikaneliö, sillä sivuluokka $(0,3) + \langle(1,-1)\rangle$ sisältää alkiot 7, 6, 5, 9, 8 ja $7+6+5+9+8 = 35 \neq 60$, missä 60 on taikasumman arvo kertaluvun viisi taikaneliössä.

16	23	0	**7**	14
22	4	**6**	13	15
3	**5**	12	19	21
9	11	18	20	2
10	17	24	1	**8**

Määritelmä 3.10. *Katkeavaksi diagonaaliksi* sanotaan lävistäjää, joka muodostuu diagonaalisesti pää- tai sivudiagonaalin ylä- tai alapuolelle yhden tai useamman ruudun erolla, ja joka sisältää neliön kertaluvun verran alkioita.

Katkeavaa diagonaalia voi visualisoida esimerkiksi piirtämällä kaksi samanlaista neliötä rinnakkain tai vaihtoehtoisesti allekkain ja aloittaa diagonaalisesti eteneminen toisesta neliöstä, jatkaen toisen neliön puolelle, kunnes muodostuu diagonaali, joka sisältää neliön kertaluvun osoittaman määrän alkioita. Havainnollistetaan tätä seuraavaksi esimerkkikuvien avulla.

Esimerkki 3.11. Alla olevassa neliössä kirjaimella X merkityt alkiot muodostavat katkeavan diagonaalin.

X	o	o	o
o	o	o	X
o	o	X	o
o	X	o	o

Asettamalla kaksi identtistä neliötä rinnakkain, ja etenemällä diagonaalisesti toisesta neliöstä toiseen neliöön, niin saadaan yksi katkeava diagonaali. Vertaamalla nyt kirjaimella X merkittyjä ruutuja edellä olevaan kuvaan, katkeavan diagonaalin idea voi hahmottua selkeämmin.

o	o	o	o
o	o	o	X
o	o	X	o
o	X	o	o

X	o	o	o
o	o	o	o
o	o	o	o
o	o	o	o

Esimerkki 3.12. Alla olevassa taikaneliössä katkeavia diagonaaleja ovat esimerkiksi 8, 12, 16, 20, 4; 19, 1, 13, 20, 7 ja 14, 21, 8, 15, 2.

0	23	(16)	[14]	**7**
19	(12)	5	3	[21]
([8])	**1**	24	17	10
22	[15]	**13**	6	(4)
11	9	[2]	(**20**)	18

Määritelmä 3.13. Taikaneliö on *yleisdiagonaalinen taikaneliö*, jos kaikkien rivien, sarakkeiden, pää- ja sivudiagonaalien sekä katkeavien diagonaalien sisältämät luvut summautuvat taikasummaksi.

Esimerkki 3.14. Esimerkin 3.5 taikaneliö on yleisdiagonaalinen taikaneliö.

Aliavaruuksien $\langle(1,1)\rangle$ ja $\langle(1,-1)\rangle$ sivuluokat sisältävät neliön pää- ja sivudiagonaalit, sekä kaikki katkeavat diagonaalit kertaluvun $q = p$ neliöissä. Siispä kertaluvun $q = p$ lineaarinen taikaneliö on yleisdiagonaalinen taikaneliö.

Lause 3.15. *Kaikki kertaluvun $q = p$ lineaariset taikaneliöt ovat yleisdiagonaalisia taikaneliöitä.*

Todistus. Äärellinen kunta $\mathbb{F} \cong \mathbb{Z}_p$ on syklinen yhteenlaskun suhteen modulo p, joten aliavaruuksien $\langle(1,1)\rangle$ ja $\langle(1,-1)\rangle$ sivuluokat sisältävät taikaneliön pää- ja sivudiagonaalit sekä kaikki katkeavat diagonaalit. Lineaarisen taikaneliön määritelmästä seuraa, että aliavaruuksien $\langle(1,1)\rangle$ ja $\langle(1,-1)\rangle$ sivuluokkien sisältämät alkiot summautuvat taikasummaksi, joten kertaluvun $q = p$ lineaarinen taikaneliö on yleisdiagonaalinen taikaneliö. □

Erilaisia taikaneliöitä saadaan kiertämällä ja peilaamalla ruudukkoa. Tämä pätee yleisesti kaikille taikaneliöille mukaan lukien lineaariset ja yleisdiagonaaliset taikaneliöt. Yhdestä taikaneliöstä saadaan muodostettua kahdeksan taikaneliötä. Alkuperäisen taikaneliön lisäksi saadaan seitsemän uutta symmetriaan perustuvaa taikaneliötä, sillä neliön symmetriaryhmään sisältyy identtisen kuvauksen lisäksi kolme kiertoa ja neljä peilausta.

Esimerkki 3.16. Tässä tutkielmassa käytetyin merkinnöin Lo Shu -neliötä vastaa ensimmäinen taikaneliö vasemmalta katsoen. Muut ylemmän rivin taikaneliöt on saatu kiertämällä ja alemman rivin taikaneliöt peilaamalla alkuperäistä taikaneliötä.

3	8	1
2	4	6
7	0	5

7	2	3
0	4	8
5	6	1

5	0	7
6	4	2
1	8	3

1	6	5
8	4	0
3	2	7

5	6	1
0	4	8
7	2	3

7	0	5
2	4	6
3	8	1

1	8	3
6	4	2
5	0	7

3	2	7
8	4	0
1	6	5

On hyvä huomioida, että edellä esiintyneiden kertaluvun kolme taikaneliöiden lisäksi, ei ole olemassa muita tämän kertaluvun taikaneliöitä. Mikään näistä kahdeksasta taikaneliöstä ei täytä lineaarisen taikaneliön, eikä myöskään yleisdiagonaalisen taikaneliön ehtoja. Näin ollen lineaarisia ja yleisdiagonaalisia taikaneliöitä löytyy vain kertaluvusta kolme eteenpäin.

Yleisdiagonaalisten taikaneliöiden tapauksessa kiertojen ja peilausten lisäksi uusia yleisdiagonaalisia taikaneliöitä voidaan muodostaa myös rivien ja sarakkeiden syklisellä permutaatiolla. Rivejä ja sarakkeita voidaan vierittää vasemmalta oikealle tai ylhäältä alas sekä näistä tietenkin myös vastakkaisiin suuntiin. Syklisen permutoinnin vuoksi kahdesta katkeavasta diagonaalista muodostuvat taikaneliön lävistäjät, ja lävistäjillä olevat alkiot muodostavat vuorostaan kaksi katkeavaa diagonaalia. Näin ollen, jos alkuperäisellä taikaneliöllä on ollut yleisdiagonaalisen taikaneliön ominaisuudet, permutoinnin jälkeisellä taikaneliöllä on edelleen nämä ominaisuudet. On kuitenkin huomioitava, että tämä ominaisuus ei ole yleistettävissä kaikille taikaneliöille.

Esimerkki 3.17. Vasemmanpuoleinen yleisdiagonaalinen taikaneliö on saatu esimerkin 3.5 taikaneliöstä vierittämällä sarakkeita yhden kerran oikealle. Oikeanpuoleinen yleisdiagonaalinen taikaneliö on puolestaan saatu vierittämällä saman taikaneliön rivejä kaksi kertaa alaspäin.

7	0	23	16	14
21	19	12	5	3
10	8	1	24	17
4	22	15	13	6
18	11	9	2	20

22	15	13	6	4
11	9	2	20	18
0	23	16	14	7
19	12	5	3	21
8	1	24	17	10

4 Lineaaristen taikaneliöiden konstruointi ja niiden olemassaolo

Pienen kertaluvun taikaneliöitä on helpohkoa laatia, mutta luonnistuuko lineaaristen taikaneliöiden laatiminen yhtä hyvin. Entäpä jos neliön kertalukua aina vain kasvatetaan?

Seuraavaksi esitetään menetelmä, jolla kertaluvun $q = p$ lineaarisia taikaneliöitä voidaan konstruoida suhteellisen yksinkertaisella tavalla. Lisäksi myöhemmin tässä luvussa osoitetaan, että lineaarisia taikaneliöitä on olemassa, kun $q = p > 3$.

4.1 Lineaaristen taikaneliöiden konstruointi

On mahdollista määritellä kuvaus, jolla saadaan kertaluvun $q = p$ taikaneliön alkioille $\{0, 1, \ldots, q^2 - 1\}$ yksikäsitteinen sijainti taikaneliössä. Tätä kuvausta varten, jokainen taikaneliön alkio $\lambda \in \{0, 1, \ldots, q^2 - 1\}$ on muutettava q-järjestelmään ja esitettävä se $\mathbb{F}^2$:n alkiona. Tätä aihetta on jo käsitelty esimerkissä 2.38, mutta yleistetään sama teoria nyt kertaluvun q taikaneliölle.

Määritelmä 4.1. Olkoon taikaneliö kertalukua $q = p$. Tällöin jokainen taikaneliön alkio $\lambda \in \{0, 1, \ldots, q^2 - 1\}$ voidaan esittää q-kantaisen lukujärjestelmän alkiona siten, että

$$\lambda = \lambda_q \cdot q + \lambda_1 \cdot 1,$$

missä $\lambda_q = \lfloor \lambda / q \rfloor$ ja λ_1 on jakoyhtälön jakojäännös.

Kokonaisluku λ voidaan kirjoittaa vektorina siten, että $\lambda = (\lambda_q, \lambda_1)$. Koska $\lambda_q, \lambda_1 \in \mathbb{F} = \{0, 1, \ldots, q - 1\}$, niin $\lambda = (\lambda_q, \lambda_1) \in \mathbb{F}^2$.

Nyt, kun taikaneliön sisältämät kokonaisluvut saadaan esitettyä q-järjestelmässä halutussa vektorimuodossa, on mahdollista edetä kuvaukseen T. Kuvaus T tuottaa lineaarisen taikaneliön määrittämällä taikaneliön alkiolle yksikäsitteisen sijainnin taikaneliössä.

Määritelmä 4.2. Olkoot A, B, C ja D skalaareja joukossa $\mathbb{Z}_p$. Nyt kertaluvun $q = p$ neliölle voidaan määritellä kuvaus $T: \{0, 1, \ldots, q^2 - 1\} \to \mathbb{F}^2$ siten, että

$$T(\lambda) = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} \lambda_q \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} A\lambda_q + B\lambda_1 \\ C\lambda_q + D\lambda_1 \end{pmatrix}.$$

Kuvaus $T(\lambda)$ tuottaa 2×1 -matriisin, missä ensimmäinen rivi kertoo millä rivillä, ja toinen, missä sarakkeessa alkio λ sijaitsee kyseisessä neliössä.

Lause 4.3. *Kuvaus $T(\lambda)$ määrittää kertaluvun $q = p$ lineaarisen taikaneliön, jos skalaarit A, B, C, D, $A \pm C$, $B \pm D$ ovat nollasta eroavia $\mathbb{Z}_p$:ssä, ja jos matriisi $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ on kääntyvä $\mathbb{Z}_p$:ssä.*

Todistus. Olkoon S kuvauksen T tuottama neliö. Koska matriisi $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ oletetaan kääntyväksi, kuvaus $T(\lambda)$ määrittää jokaiselle alkiolle λ yksikäsitteisen sijainnin tässä neliössä. Siirrytään seuraavaksi tarkastelemaan neliön S taikasummia. Olkoon $\mu \in \mathbb{F} \cong \mathbb{Z}_p$ neliön μ:s rivi. Nyt tällä rivillä olevat alkiot $\lambda = (\lambda_q, \lambda_1)$ ovat yhtälön $A\lambda_q + B\lambda_1 = \mu$ ratkaisuja. Koska sekä A että B ovat nollasta eroavia, yhtälölle $A\lambda_q = \mu - B\lambda_1$ on olemassa yksikäsitteinen ratkaisu λ_q jokaisella mahdollisella λ_1:n arvolla. Kun neliön alkio λ kirjoitetaan määritelmän 4.1 mukaisesti, sekä λ_q ja λ_1 saavat arvot $\{0, 1, \ldots, q-1\}$ täsmälleen kerran rivillä μ. Siispä, kun μ:nnen rivin alkiot summataan yhteen, summaksi saadaan

$$(0 + 1 + \cdots + (q-1)) \cdot q + (0 + 1 + \cdots + (q-1)) \cdot 1$$

$$= \frac{q^2(q-1)}{2} + \frac{q(q-1)}{2} = \frac{q(q^2-1)}{2},$$

mikä vastaa aiemmin taikasummalle annettua määritelmää 3.4. Samalla tavoin voidaan osoittaa, että neliön S sarakkeiden alkiot summautuvat taikasummaksi, kun A ja B korvataan skalaareilla C ja D.

Lisäksi on vielä osoitettava, että aliavaruuksien $\langle(1,1)\rangle$ ja $\langle(1,-1)\rangle$ sivuluokkien sisältämät alkiot summautuvat taikasummaksi.
Olkoon $\mu_1, \mu_2 \in \mathbb{F} \cong \mathbb{Z}_p$. Tällöin alkiolle λ, joka sijaitsee sivuluokassa $(\mu_1, \mu_2) + \langle(1,1)\rangle$, on oltava voimassa ehto

$$T(\lambda) = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} + \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}$$

jollakin $\alpha \in \mathbb{F} \cong \mathbb{Z}_p$. Lisäksi kuvauksen T määritelmän 4.2 nojalla pätee, että

$$\mu_1 = A\lambda_q + B\lambda_1 \text{ ja } \mu_2 = C\lambda_q + D\lambda_1,$$

jolloin

$$\mu_1 - \mu_2 = (A - C)\lambda_q + (B - D)\lambda_1.$$

Koska $A-C$ ja $B-D \neq 0$, niin on olemassa yksikäsitteinen ratkaisu λ_q jokaisella λ_1:n arvolla, jolloin $\begin{pmatrix}\mu_1\\ \mu_2\end{pmatrix}$ ja siten myös $\begin{pmatrix}\mu_1\\ \mu_2\end{pmatrix} + \begin{pmatrix}\alpha\\ \alpha\end{pmatrix}$ on yksikäsitteinen jokaiselle sivuluokan alkiolle. Tällöin saadaan samanlainen väite kuin edellä, jolloin tarkasteltiin neliön S rivien sisältäminen alkioiden taikasummia. Voidaan siis aikaisempien tietojen pohjalta todeta, että $\langle(1,1)\rangle$ sivuluokkien sisältämät alkiot summautuvat taikasummaksi. Vastaavalla tavalla voidaan käsitellä $\langle(1,-1)\rangle$ sivuluokat, jolloin päädytään tilanteeseen

$$\mu_1 - \mu_2 = (A + C)\lambda_q + (B + D)\lambda_1,$$

missä nyt $A+C$ ja $B+D \neq 0$. Näin ollen kuvauksen T tuottama neliö S on lineaarinen taikaneliö. □

Katsotaan seuraavaksi vielä esimerkin avulla, miten taikaneliön rivien, sarakkeiden, lävistäjien tai katkeavien diagonaalien sisältämien alkioiden summia lasketaan, jos alkiot on esitetty vektorimuodossa $\lambda = (\lambda_q, \lambda_1)$.

Esimerkki 4.4. Ohessa on esitetty esimerkissä 3.5 esiintynyt taikaneliö niin, että kokonaisluvut $\lambda \in \{0, 1, \ldots, 24\}$ on esitetty vektorina (λ_5, λ_1).

(0,0)	(4,3)	(3,1)	(2,4)	(1,2)
(3,4)	(2,2)	(1,0)	(0,3)	(4,1)
(1,3)	(0,1)	(4,4)	(3,2)	(2,0)
(4,2)	(3,0)	(2,3)	(1,1)	(0,4)
(2,1)	(1,4)	(0,2)	(4,0)	(3,3)

Jokainen rivi, sarake, lävistäjä ja katkeava diagonaali sisältää alkiot $\lambda_5, \lambda_1 \in \{0, 1, 2, 3, 4\}$ täsmälleen kerran. Sivudiagonaalilla sijaitsee alkiot

$$(1, 2), (0, 3), (4, 4), (3, 0), (2, 1),$$

ja koska esimerkiksi alkio $(1, 2) = 1 \cdot 5 + 2 \cdot 1$, kaikkien sivudiagonaalilla sijaitsevien alkioiden summaksi saadaan

$$(1 + 0 + 4 + 3 + 2)5 + (2 + 3 + 4 + 0 + 1)1.$$

Käyttäen hyödyksi aritmeettista sarjaa, summalauseke saadaan muotoon

$$\frac{5(0+4)}{2}\cdot 5+\frac{5(0+4)}{2}\cdot 1=\frac{5^2\cdot 4}{2}+\frac{5\cdot 4}{2}=\frac{5(5^2-1)}{2}=60.$$

Sivudiagonaalilla sijaitsevien alkioiden summaksi saadaan siis 60, joka vastaa taikasumman arvoa kertaluvun viisi taikaneliössä.

Seuraavassa esimerkissä on laadittu kertaluvun viisi ja seitsemän lineaariset taikaneliöt lauseen 4.3 mukaisesti.

Esimerkki 4.5. (a) Kuvaus $T(\lambda)=\begin{pmatrix}4&2\\2&4\end{pmatrix}\begin{pmatrix}\lambda_5\\\lambda_1\end{pmatrix}$ määrittää kertaluvun viisi lineaarisen taikaneliön, missä $\lambda\in\{0,1,\ldots,24\}$.

0	22	19	11	8
14	6	3	20	17
23	15	12	9	1
7	4	21	18	10
16	13	5	2	24

Esimerkiksi alkioiden 13 ja 20 sijainnit tässä taikaneliössä on saatu seuraavasti:

$$T(13)=\begin{pmatrix}4&2\\2&4\end{pmatrix}\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}4\\1\end{pmatrix}\quad\text{ja}\quad T(20)=\begin{pmatrix}4&2\\2&4\end{pmatrix}\begin{pmatrix}4\\0\end{pmatrix}=\begin{pmatrix}1\\3\end{pmatrix}.$$

(b) Kuvaus $T(\lambda)=\begin{pmatrix}2&6\\1&2\end{pmatrix}\begin{pmatrix}\lambda_7\\\lambda_1\end{pmatrix}$ määrittää kertaluvun seitsemän lineaarisen taikaneliön, missä $\lambda\in\{0,1,\ldots,48\}$.

0	27	47	18	38	9	29
46	17	37	8	28	6	26
36	7	34	5	25	45	16
33	4	24	44	15	35	13
23	43	14	41	12	32	3
20	40	11	31	2	22	42
10	30	1	21	48	19	39

4.2 Lineaaristen taikaneliöiden olemassaolo

Lineaaristen taikaneliöiden konstruointi kuvauksen T avulla tuottaa ominaisuuksiltaan toivotun lopputuloksen, mikäli matriisit A, B, C ja D toteuttavat niille lauseessa 4.3 asetetut ehdot. Kertaluvun $q = p > 3$ lineaarisia taikaneliöitä on aina mahdollista konstruoida edellä esitetyllä tavalla.

Lause 4.6. *Kertaluvun $q = p > 3$ lineaarinen taikaneliö on aina olemassa.*

Todistus. Lauseen todistamiseksi on näytettävä, että kertaluvun $q = p > 3$ lineaarisen taikaneliön konstruoimiseksi löytyvät sellaiset skalaarit A, B, C ja D, jotka toteuttavat niille asetetut ehdot. Kun $p > 3$, määritellään $A = 2$, $B = C = 1$ ja $D = -\frac{1}{2}$. Näin kuvauksen T kerroinmatriisiksi saadaan $\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & -\frac{1}{2} \end{pmatrix}$. Matriisi on kääntyvä $\mathbb{Z}_p$:ssä, kun $p > 3$, sillä $\det \begin{pmatrix} 2 & 1 \\ 1 & -\frac{1}{2} \end{pmatrix} = -2 \neq 0$. Tästä seuraa, että lineaarisia taikaneliöitä löytyy kertaluvusta $q = p > 3$ eteenpäin. □

Esimerkki 4.7. Kuvaus $T(\lambda) = \begin{pmatrix} 2 & 1 \\ 1 & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} \lambda_5 \\ \lambda_1 \end{pmatrix}$ määrittää kertaluvun viisi lineaarisen taikaneliön, missä $\lambda \in \{0, 1, \ldots, 24\}$.

0	19	8	22	11
23	12	1	15	9
16	5	24	13	2
14	3	17	6	20
7	21	10	4	18

Nyt esimerkiksi alkion 3 sijainti saadaan seuraavasti:

$$T(3) = \begin{pmatrix} 2 & 1 \\ 1 & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ -\frac{3}{2} \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}.$$

Tässä siis

$$-\frac{3}{2} \equiv -\frac{8}{2} = -4$$

ja

$$-4 \equiv 1 \pmod 5.$$

Kuvaus T ei sovellu kertaluvun $q = p \leq 3$ lineaarisen taikaneliön konstruointiin kahdesta syystä. Ensinnäkin kertaluvun kolme taikaneliö on pienin mahdollinen taikaneliö, joten kertaluvun kaksi lineaarista taikaneliötä ei siten voi olla olemassa. Toisaalta tapauksen $q = p = 3$ mahdottomuus on käyty läpi esimerkin 3.16 yhteydessä.

Viitteet

[1] Block S. S., Tavares, A. S., *Before Sudoku, The World of Magic Squares*, Oxford University Press, 2009.

[2] Hyry E., *Algebra 1* [Luentomuistiinpanot] Tampereen yliopisto, 2010.

[3] Lorch J., *Magic Squares and Sudoku*, The American Mathematical Monthly, Vol. 119. No. 9 (November 2012). pp. 759-770.

[4] Pickover C. A., *The Zen of Magic Squares, Circles, and Stars*, Princeton, New Jersey; Princeton University Press, 2003.

[5] Rinta-aho M., *Äärelliset kunnat* [Luentomoniste] Oulun yliopisto, 2011. Saatavissa osoitteessa: http://cc.oulu.fi/m̃rinta/FF/FF_luento.pdf [viitattu 3.6.2014].

[6] Rotman J., *Advanced Modern Algebra*. 2:nd printing. Prentice Hall, 2003.

[7] Rotman J., *A First Course in Abstract Algebra*. 3:rd edition. University of Illinois at Urbana-Champaign. Prentice Hall, 2005.